PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-235340
(43)Date of publication of application : 29.08.2000

(51)Int.Cl. G09C 1/00
G06F 13/00

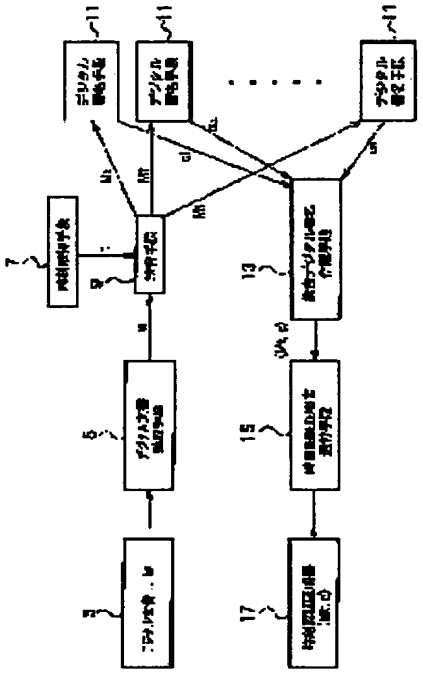
(21)Application number : 11-035761
(22)Date of filing : 15.02.1999

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : TAKURA AKIRA
ONO SATOSHI

(54) TIME AUTHENTICATION DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a safe and reliable time authentication device for exactly preventing falsification of a time stamp by writing a digital signature with divided plural partial secret keys.

SOLUTION: A digital document (M) 3 prepared by an author is received by a digital document receiving means 5 and coupled to time information (t) from a time acquisition means 7 by a coupling means 9, and a digital document with one time stamp Mt is prepared, and this digital document with time stamp Mt is forwarded to plural digital signature means 11 to prepare digital signatures independently of each other. And, an integrated digital signature preparing means 13 receives the plural digital signatures independently prepared by the plural digital signature preparing means 11 and combines them to prepare an integrated digital signatures (c), and a time authentication certificate forwarding means 15 sends a set of the digital document with time stamp Mt and the integrated digital signature (c) to the author as a time authentication certificate (Mt, c) 17.



LEGAL STATUS

[Date of request for examination]	15.02.1999
[Date of sending the examiner's decision of rejection]	01.07.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3515408
[Date of registration]	23.01.2004
[Number of appeal against examiner's decision of rejection]	2003-14754
[Date of requesting appeal against examiner's decision of rejection]	31.07.2003

NTT-1733

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－235340
（P2000－235340A）
(43)公開日　平成12年８月29日(2000.8.29)

(51)Int.Cl.⁷	識別記号	Ｆ Ｉ	テーマコード（参考）
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ　５Ｂ０８９
			６４０Ｚ　５Ｊ１０４
Ｇ０６Ｆ　13/00	３５４	Ｇ０６Ｆ　13/00	３５４Ｚ

審査請求　有　　請求項の数11　ＯＬ　（全 20 頁）

(21)出願番号　特願平11－35761

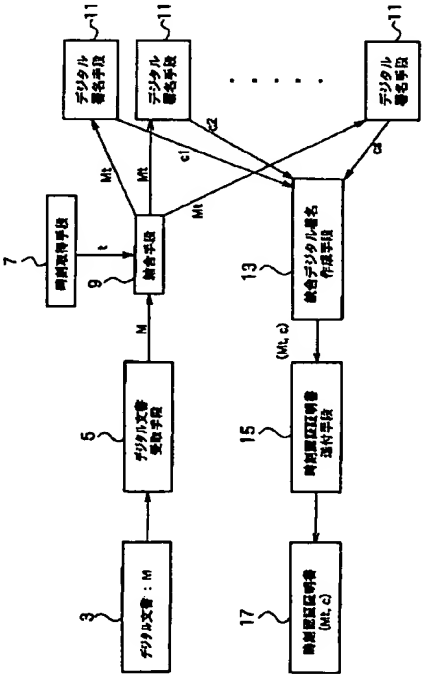
(22)出願日　平成11年２月15日(1999.2.15)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　田倉　昭
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　小野　論
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外１名）

Ｆターム(参考)　5B089 JA31 JB11 KA17 KC58
5J104 AA09 AA11 LA03 LA07 PA07

(54)【発明の名称】　時刻認証装置

(57)【要約】
【課題】　複数の分割された部分的な秘密鍵でデジタル署名を行うことにより時刻印の偽造を適確に防止し、安全で信頼のおける時刻認証装置を提供する。
【解決手段】　著者が作成したデジタル文書（Ｍ）３はデジタル文書受取手段５で受け取られ、結合手段９において時刻取得手段７からの時刻情報ｔを結合されて、１つの時刻印付デジタル文書Ｍｔが作成され、この時刻印付デジタル文書Ｍｔは複数のデジタル署名手段１１に送付され、各々独立にデジタル署名を作成され、この複数のデジタル署名手段１１で独立に作成された複数のデジタル署名を統合デジタル署名作成手段１３で受け取り結合して、統合デジタル署名ｃを作成し、時刻認証証明書送付手段１５において時刻印付デジタル文書Ｍｔと統合デジタル署名ｃの組を時刻認証証明書（Ｍｔ，ｃ）１７として著者に送付する。



1

【特許請求の範囲】

【請求項１】　著者が作成したデジタル文書Ｍを受け取る文書受取手段と、

時刻情報ｔを取得する時刻取得手段と、

該時刻取得手段で取得した時刻情報ｔを前記デジタル文書Ｍに結合して、１つの時刻印付デジタル文書Ｍｔを作成する結合手段と、

前記時刻印付デジタル文書Ｍｔを受け取って、各々独立にデジタル署名を作成する複数のデジタル署名手段と、

該複数のデジタル署名手段で独立に作成された複数のデジタル署名を受け取り結合して、統合デジタル署名ｃを作成する統合デジタル署名作成手段と、

前記時刻印付デジタル文書Ｍｔおよび統合デジタル署名ｃの組を時刻認証証明書として著者に送付する時刻認証証明書送付手段とを有することを特徴とする時刻認証装置。

【請求項２】　前記結合手段は、前記時刻印付デジタル文書Ｍｔを前記複数のデジタル署名手段に送付する時刻印付デジタル文書送付手段と、前記複数のデジタル署名手段から送付される複数のデジタル署名を受け取るデジタル署名受取手段とを有し、

前記複数のデジタル署名手段の各々は、前記時刻印付デジタル文書送付手段から送付される時刻印付デジタル文書Ｍｔを受け取る時刻印付デジタル文書受取手段と、この受け取った時刻印付デジタル文書Ｍｔに対して各々独立にデジタル署名を作成するデジタル署名作成手段と、この作成されたデジタル署名を前記デジタル署名受取手段に送付する署名送付手段とを有することを特徴とする請求項１記載の時刻認証装置。

【請求項３】　著者が作成したデジタル文書Ｍを受け取り、このデジタル文書Ｍに認証要求者が必要とする認証の有効期間情報Ｐを結合するとともにデジタル署名を作成し、更に公開鍵証明書Ｃを加えた組からなる有効期間付署名要求（ＭＰ，Ｑ，Ｃ）を送付する有効期間付き署名要求手段、および該有効期間付き署名要求手段から送付される前記有効期間付署名要求（ＭＰ，Ｑ，Ｃ）を受け取り、該有効期間付署名要求（ＭＰ，Ｑ，Ｃ）が正規の契約者からの要求であることを検証し、デジタル文書Ｍに時刻情報ｔを結合してデジタル署名した時刻認証証明書（Ｍｔ，ｃ）を作成する時刻認証手段を有する時刻認証装置であって、

前記有効期間付き署名要求手段は、

著者が作成したデジタル文書Ｍを受け取るデジタル文書受取手段と、

公開鍵暗号方式における公開鍵と秘密鍵の組を作成し、この作成した公開鍵を前記時刻認証手段に送付する鍵作成手段と、

前記デジタル文書受取手段が受け取ったデジタル文書Ｍに認証要求者が必要とする認証の有効期間Ｐを結合して、情報ＭＰを作成する有効期間結合手段と、

2

前記情報ＭＰに対して秘密鍵を用いてデジタル署名Ｑを作成するデジタル署名手段と、

前記情報ＭＰ、デジタル署名Ｑ、および時刻認証手段から受け取った公開鍵証明書Ｃの組を有効期間付署名要求（ＭＰ，Ｑ，Ｃ）として時刻認証手段に送付する有効期間付要求送付手段とを有し、

前記時刻認証手段は、

前記有効期間付き署名要求手段から送付される前記公開鍵を受け取り、該有効期間付き署名要求手段からの要求に応じて該公開鍵に対するデジタル署名を該時刻認証手段の秘密鍵で作成し、該公開鍵とこの作成されたデジタル署名を組にした公開鍵証明書Ｃを前記有効期間付き署名要求手段に送付する公開鍵証明書返送手段と、

前記有効期間付き署名要求手段から送付される有効期間付署名要求（ＭＰ，Ｑ，Ｃ）を受け取る有効期間付署名要求受取手段と、

この受け取った有効期間付署名要求（ＭＰ，Ｑ，Ｃ）に含まれるデジタル署名Ｑおよび公開鍵証明書Ｃを検証して、署名要求者が正規の契約者であることを確認する有効期間付署名検証手段と、

時刻情報ｔを取得する時刻取得手段と、

前記有効期間付署名検証手段による検証結果が有効である場合、前記時刻取得手段で取得した時刻情報ｔが前記有効期間付署名要求（ＭＰ，Ｑ，Ｃ）に含まれる有効期間Ｐに含まれるか否かを検証する有効期間内時刻情報検証手段と、

該有効期間内時刻情報検証手段による検証により時刻情報ｔが有効期間Ｐに含まれる場合のみ、前記時刻取得手段で取得した時刻情報ｔを前記有効期間付署名要求（ＭＰ，Ｑ，Ｃ）に含まれるデジタル文書Ｍに結合して、時刻印付デジタル文書Ｍｔを作成する時刻情報結合手段と、

前記時刻印付デジタル文書Ｍｔを受け取って、各々独立にデジタル署名を作成する複数のデジタル署名手段と、

該複数のデジタル署名手段で独立に作成された複数のデジタル署名を受け取り結合して、統合デジタル署名ｃを作成する統合デジタル署名作成手段と、

前記時刻印付デジタル文書Ｍｔおよび統合デジタル署名ｃの組を時刻認証証明書（Ｍｔ，ｃ）として著者に送付する時刻認証証明書送付手段とを有することを特徴とする時刻認証装置。

【請求項４】　前記時刻情報結合手段は、前記時刻印付デジタル文書Ｍｔを前記複数のデジタル署名手段に送付する時刻印付デジタル文書送付手段と、前記複数のデジタル署名手段から送付される複数のデジタル署名を受け取るデジタル署名受取手段とを有し、

前記複数のデジタル署名手段の各々は、前記時刻印付デジタル文書送付手段から送付される時刻印付デジタル文書Ｍｔを受け取る時刻印付デジタル文書受取手段と、この受け取った時刻印付デジタル文書Ｍｔに対して各々独

立にデジタル署名を作成するデジタル署名作成手段と、この作成されたデジタル署名を前記デジタル署名受取手段に送付する署名送付手段とを有することを特徴とする請求項３記載の時刻認証装置。

【請求項５】　前記複数のデジタル署名手段が正常に動作しているか否を確認するための問い合わせを定期的に各デジタル署名手段に対して行い、この確認結果を前記結合手段および統合デジタル署名作成手段に供給する動作確認手段を更に有し、

前記結合手段は、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書Ｍｔを送付し、

前記統合デジタル署名作成手段は、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取るように構成されていることを特徴とする請求項１記載の時刻認証装置。

【請求項６】　前記複数のデジタル署名手段が正常に動作しているか否を確認するための問い合わせを定期的に各デジタル署名手段に対して行い、この確認結果を前記時刻印付デジタル文書送付手段およびデジタル署名受取手段に供給する動作確認手段を更に有し、

前記時刻印付デジタル文書送付手段は、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書Ｍｔを送付し、

前記デジタル署名受取手段は、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取るように構成されていることを特徴とする請求項２記載の時刻認証装置。

【請求項７】　公開鍵暗号方式における公開鍵Ｋｐと秘密鍵Ｋｓの組を作成し、この作成された秘密鍵Ｋｓを分割して、前記複数のデジタル署名手段の数の数値の和として表現し、この各数値を１つずつ前記複数のデジタル署名手段の各々に配付し、配付完了後、分割前の秘密鍵を削除する鍵作成・分配手段を更に有し、

前記複数のデジタル署名手段の各々は、前記鍵作成・分配手段からそれぞれ配付された秘密鍵を保持し、該秘密鍵を用いた公開鍵暗号方式で前記結合手段から配付された時刻印付デジタル文書Ｍｔに対するデジタル署名を作成し、この各デジタル署名手段からの複数のデジタル署名を前記統合デジタル署名作成手段で結合して統合デジタル署名ｃを作成し、前記時刻認証証明書送付手段で時刻印付デジタル文書Ｍｔ、統合デジタル署名ｃ、および公開鍵Ｋｐを組にして時刻認証証明書（Ｍｔ，ｃ，Ｋｐ）として著者に送付するように構成されていることを特徴とする請求項１記載の時刻認証装置。

【請求項８】　前記複数のデジタル署名手段が正常に動作しているか否を確認するための問い合わせを定期的に各デジタル署名手段に対して行い、この確認結果を前記結合手段、統合デジタル署名作成手段、および鍵作成・分配手段に供給する動作確認手段を更に有し、

前記鍵作成・分配手段は、前記動作確認手段から正常に動作していないデジタル署名手段があるという動作確認結果を受け取ると、新たな公開鍵および秘密鍵を作成し、この新たに作成した秘密鍵を前記複数のデジタル署名手段の数の和に分割し、この分割して得られた秘密鍵を各デジタル署名手段に１つずつ配付し、前記結合手段は、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書Ｍｔを送付し、この時刻印付デジタル文書Ｍｔを送付された各デジタル署名手段は前記鍵作成・分配手段から配付された秘密鍵を用いて前記結合手段から配付された時刻印付デジタル文書Ｍｔに対するデジタル署名を作成し、前記統合デジタル署名作成手段は、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取り、この受け取ったデジタル署名を前記統合デジタル署名作成手段で結合して統合デジタル署名ｃを作成し、前記時刻認証証明書送付手段で時刻印付デジタル文書Ｍｔ、統合デジタル署名ｃ、および公開鍵Ｋｐを組にして時刻認証証明書（Ｍｔ，ｃ，Ｋｐ）として著者に送付するように構成されていることを特徴とする請求項７記載の時刻認証装置。

【請求項９】　前記結合手段は、前記時刻印付デジタル文書Ｍｔを前記複数のデジタル署名手段に送付する時刻印付デジタル文書送付手段と、前記複数のデジタル署名手段から送付される複数のデジタル署名を受け取るデジタル署名受取手段とを有することを特徴とする請求項７記載の時刻認証装置。

【請求項１０】　前記デジタル署名手段の各々は、独自に時刻情報ｔ′を取得する時刻取得手段を更に有し、前記時刻印付デジタル文書Ｍｔを受信すると、該時刻印付デジタル文書Ｍｔから直ちに時刻情報ｔを取得し、この時刻情報ｔと前記独自に取得した時刻情報ｔ′とを比較し、両者の差が所定の許容時間差以内であるときのみ、デジタル署名を作成するように構成されていることを特徴とする請求項２記載の時刻認証装置。

【請求項１１】　公開鍵暗号方式における公開鍵Ｋｐ２と秘密鍵Ｋｓ２の組を作成し、この作成された秘密鍵Ｋｓ２を分割して、複数のデジタル署名手段の数の数値の和として表現し、この各数値を１つずつ複数のデジタル署名手段の各々に配付し、配付完了後、分割前の秘密鍵を削除する鍵作成・分配手段を更に有し、

前記時刻認証手段は、前記複数のデジタル署名手段が正常に動作しているか否を確認するための問い合わせを定期的に各デジタル署名手段に対して行う動作確認手段を更に有し、

前記デジタル署名手段の各々は、独自に時刻情報ｔ′を取得する時刻取得手段を更に有し、前記時刻印付デジタル文書Ｍｔを受信すると、該時刻印付デジタル文書Ｍｔ

から直ちに時刻情報ｔを取得し、この時刻情報ｔと前記独自に取得した時刻情報ｔ′とを比較し、両者の差が所定の許容時間差以内であるときのみ、デジタル署名を作成するように構成され、
前記鍵作成・分配手段は、前記動作確認手段から正常に動作していないデジタル署名手段があるという動作確認結果を受け取ると、新たな公開鍵および秘密鍵を作成し、この新たに作成した秘密鍵を前記複数のデジタル署名手段の数の和に分割し、この分割して得られた秘密鍵を各デジタル署名手段に１つずつ配付し、前記結合手段は、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書Ｍｔを送付し、デジタル署名手段は、時刻印付デジタル文書Ｍｔを受信すると、該時刻印付デジタル文書Ｍｔから直ちに時刻情報ｔを取得し、この時刻情報ｔと独自に取得した時刻情報ｔ′とを比較し、両者の差が所定の許容時間差以内であるときのみ、鍵作成・分配手段から配付された秘密鍵を用いて前記結合手段から配付された時刻印付デジタル文書Ｍｔに対するデジタル署名を作成し、統合デジタル署名作成手段は、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取り、この受け取ったデジタル署名を統合デジタル署名作成手段で結合して統合デジタル署名ｃを作成し、時刻認証証明書送付手段で時刻印付デジタル文書Ｍｔ、統合デジタル署名ｃ、および公開鍵Ｋｐ２を組にして時刻認証証明書（Ｍｔ，ｃ，Ｋｐ２）として著者に送付するように構成されていることを特徴とする請求項４記載の時刻認証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、テキスト文書、画像情報、音声情報等を含むデジタル文書に時刻印を押すことにより時刻印を押された時点以降にデジタル文書が変更されてなく、確かに時刻印が押された時点で対象とするデジタル文書が存在していたことを証明する時刻認証装置に関し、更に詳しくは、インターネット等の不特定多数のユーザが接続されているネットワーク上に時刻認証装置が設置されているときに、時刻認証装置の利用を許可されたユーザ以外の者が不正に時刻認証装置を利用することを防止するとともに、時刻認証証明書が不正に偽造されることを防止し得る時刻認証装置に関する。

【０００２】

【従来の技術】この種の時刻認証装置として、従来提案されている例えば特開平７－２５４８９７号「個人用日時認証装置」では、スマートカード等に時刻認証装置を組み込み、デジタル署名を行う時に時刻認証を一緒に行っている。また、特開平３－１８５５５１号「デジタル時間認証装置」では、時刻認証装置を１つのハードウェアプラットフォームとして構成し、文書の作成者がこの装置を使用して時刻認証を行っている。これらの従来の装置では、いずれも文書作成者が時刻認証を行う方式であるため、偽造し易く、第三者機関による証明でないため、信頼性が乏しい。

【０００３】また、特開平６－１４０１８号「電子的公証方法および装置」では、元の文書に対するＣＲＣ（Cyclic Redundancy Check）、パリティ、検査合計を組み合わせて圧縮文書を作成し、時刻認証を行っている。この方式で作成される圧縮文書は、現在広く暗号技術として使用されているＭＤ５やＳＨＡ－１などのハッシュ関数を用いて作成される圧縮文書と比較して同一の圧縮文書を持つデジタル文書の偽造がし易い。更に、特開平６－５０１５７４号「数値文書に確実にタイムスタンプを押す方法」では、時刻認証を行う外部機関が単独で時刻認証証明書を作成しているが、この方式は外部機関が時刻認証証明書を偽造することが容易である。

【０００４】上述した従来の欠点を補うために、従来、受け取った時刻認証要求とその外部機関が直前に発行した時刻認証証明書を結合したデジタル文書に対してハッシュ関数を適用して得られた圧縮文書にデジタル署名を行い、時刻認証証明書を作成する方法を提案しているものがある。この方法は、時刻認証外部機関が時刻認証証明書を偽造することを事実上不可能にしているが、時刻認証証明書が真正であることを証明するには、それ以前に発行した証明書のデジタル署名が必要となる。すなわち、時刻認証外部機関が発行したすべての時刻認証証明書を保存しておかないと、時刻認証証明書が真正であることを証明することができないため、膨大な記憶容量が必要となる。

【０００５】

【発明が解決しようとする課題】上述したように、従来の時刻認証装置のうち、特開平７－２５４８９７号や特開平３－１８５５５１号に提案されている従来の装置では、いずれも文書作成者が時刻認証を行う方式であるため、偽造し易く、第三者機関による証明でないため、信頼性が乏しいという問題がある。

【０００６】また、特開平６－１４０１８号のようにＣＲＣ、パリティ、検査合計を組み合わせて圧縮文書を作成し、時刻認証を行う従来の方式における圧縮文書は、同一の圧縮文書を持つデジタル文書の偽造がし易いという問題がある。

【０００７】更に、特開平６－５０１５７４号のように時刻認証を行う外部機関が単独で時刻認証証明書を作成する方式では外部機関が時刻認証証明書を偽造することが容易であるという問題がある。

【０００８】上述した従来の欠点を補うために、時刻認証要求と外部機関が直前に発行した時刻認証証明書を結合したデジタル文書にハッシュ関数を適用した圧縮文書にデジタル署名を行い、時刻認証証明書を作成する従来の方法では、時刻認証外部機関が発行したすべての時刻認証証明書を保存しておかないと、時刻認証証明書が真

正であることを証明することができないため、膨大な記憶容量が必要となり、非経済的であるという問題がある。

【０００９】また、ＩＥＴＦにおいてハッシュ関数により圧縮されたデジタル文書を外部機関に送付し、この送付されたデジタル文書に対して時刻認証証明書を作成するプロトコルの標準化が進められているが、この方法は外部機関が１ヶ所で時刻認証証明書を作成するため、時刻認証証明書の偽造の可能性および時刻認証証明書を取得することが許されていない悪意のある第三者が不正に時刻認証証明書を取得する危険性を排除することができないという問題がある。

【００１０】本発明は、上記に鑑みてなされたもので、その目的とするところは、複数の分割された部分的な秘密鍵でデジタル署名を行うことにより時刻印の偽造を適確に防止し、安全で信頼のおける時刻認証装置を提供することにある。

【００１１】

【課題を解決するための手段】上記目的を達成するため、請求項１記載の本発明は、著者が作成したデジタル文書Ｍを受け取る文書受取手段と、時刻を取得する時刻取得手段と、該時刻取得手段で取得した時刻情報ｔを前記デジタル文書Ｍに結合して、１つの時刻印付デジタル文書Ｍｔを作成する結合手段と、前記時刻印付デジタル文書Ｍｔを受け取って、各々独立にデジタル署名を作成する複数のデジタル署名手段と、該複数のデジタル署名手段で独立に作成された複数のデジタル署名を受け取り結合して、統合デジタル署名ｃを作成する統合デジタル署名作成手段と、前記時刻印付デジタル文書Ｍｔおよび統合デジタル署名ｃの組を時刻認証証明書として著者に送付する時刻認証証明書送付手段とを有することを要旨とする。

【００１２】請求項１記載の本発明にあっては、著者が作成したデジタル文書Ｍは時刻取得手段からの時刻情報ｔを結合されて、１つの時刻印付デジタル文書Ｍｔが作成され、この時刻印付デジタル文書Ｍｔは複数のデジタル署名手段に送付され、各々独立にデジタル署名を作成され、この複数のデジタル署名手段で独立に作成された複数のデジタル署名を結合して、統合デジタル署名を作成し、この統合デジタル署名および時刻印付デジタル文書の組を時刻認証証明書として著者に送付されるため、複数のデジタル署名手段による各々独自なデジタル署名により時刻印の偽造が困難であり、安全で信頼のおける時刻認証サービスが可能であるとともに、秘密鍵盗難の危険を低減することができる。また、過去に発行した時刻認証証明書を保管することもなく、記憶容量を大幅に削減し得る。

【００１３】また、請求項２記載の本発明は、請求項１記載の発明において、前記結合手段が、前記時刻印付デジタル文書Ｍｔを前記複数のデジタル署名手段に送付する時刻印付デジタル文書送付手段と、前記複数のデジタル署名手段から送付される複数のデジタル署名を受け取るデジタル署名受取手段とを有し、前記複数のデジタル署名手段の各々が、前記時刻印付デジタル文書送付手段から送付される時刻印付デジタル文書Ｍｔを受け取る時刻印付デジタル文書受取手段と、この受け取った時刻印付デジタル文書Ｍｔに対して各々独立にデジタル署名を作成するデジタル署名作成手段と、この作成されたデジタル署名を前記デジタル署名受取手段に送付する署名送付手段とを有することを要旨とする。

【００１４】請求項２記載の本発明にあっては、複数のデジタル署名手段を外部デジタル署名手段として外部に設け、結合手段からの時刻印付デジタル文書Ｍｔを時刻印付デジタル文書送付手段から外部の複数のデジタル署名手段に送付し、この複数のデジタル署名手段の各々で作成された複数のデジタル署名をデジタル署名受取手段で受け取るため、外部に設けられた複数のデジタル署名手段による各々独自なデジタル署名により時刻印の偽造が更に困難であり、安全で信頼のおける時刻認証サービスが可能である。

【００１５】更に、請求項３記載の本発明は、著者が作成したデジタル文書Ｍを受け取り、このデジタル文書Ｍに認証要求者が必要とする認証の有効期間情報Ｐを結合するとともにデジタル署名を作成し、更に公開鍵証明書Ｃを加えた組からなる有効期間付署名要求（ＭＰ，Ｑ，Ｃ）を送付する有効期間付き署名要求手段、および該有効期間付き署名要求手段から送付される前記有効期間付署名要求（ＭＰ，Ｑ，Ｃ）を受け取り、該有効期間付署名要求（ＭＰ，Ｑ，Ｃ）が正規の契約者からの要求であることを検証し、デジタル文書Ｍに時刻情報ｔを結合してデジタル署名した時刻認証証明書（Ｍｔ，ｃ）を作成する時刻認証手段を有する時刻認証装置であって、前記有効期間付き署名要求手段が、著者が作成したデジタル文書Ｍを受け取るデジタル文書受取手段と、公開鍵暗号方式における公開鍵と秘密鍵の組を作成し、この作成した公開鍵を前記時刻認証手段に送付する鍵作成手段と、前記デジタル文書受取手段が受け取ったデジタル文書Ｍに認証要求者が必要とする認証の有効期間Ｐを結合して、情報ＭＰを作成する有効期間結合手段と、前記情報ＭＰに対して秘密鍵を用いてデジタル署名Ｑを作成するデジタル署名手段と、前記情報ＭＰ、デジタル署名Ｑ、および時刻認証手段から受け取った公開鍵証明書Ｃの組を有効期間付署名要求（ＭＰ，Ｑ，Ｃ）として時刻認証手段に送付する有効期間付要求送付手段とを有し、前記時刻認証手段が、前記有効期間付き署名要求手段から送付される前記公開鍵を受け取り、該有効期間付き署名要求手段からの要求に応じて該公開鍵に対するデジタル署名を該時刻認証手段の秘密鍵で作成し、該公開鍵とこの作成されたデジタル署名を組にした公開鍵証明書Ｃを前記有効期間付き署名要求手段に送付する公開鍵証明書返

送手段と、前記有効期間付き署名要求手段から送付される有効期間付署名要求（ＭＰ，Ｑ，Ｃ）を受け取る有効期間付署名要求受取手段と、この受け取った有効期間付署名要求（ＭＰ，Ｑ，Ｃ）に含まれるデジタル署名Ｑおよび公開鍵証明書Ｃを検証して、署名要求者が正規の契約者であることを確認する有効期間付署名検証手段と、時刻情報ｔを取得する時刻取得手段と、前記有効期間付署名検証手段による検証結果が有効である場合、前記時刻取得手段で取得した時刻情報ｔが前記有効期間付署名要求（ＭＰ，Ｑ，Ｃ）に含まれる有効期間Ｐに含まれるか否かを検証する有効期間内時刻情報検証手段と、該有効期間内時刻情報検証手段による検証により時刻情報ｔが有効期間Ｐに含まれる場合のみ、前記時刻取得手段で取得した時刻情報ｔを前記有効期間付署名要求（ＭＰ，Ｑ，Ｃ）に含まれるデジタル文書Ｍに結合して、時刻印付デジタル文書Ｍｔを作成する時刻情報結合手段と、前記時刻印付デジタル文書Ｍｔを受け取って、各々独立にデジタル署名を作成する複数のデジタル署名手段と、該複数のデジタル署名手段で独立に作成された複数のデジタル署名を受け取り結合して、統合デジタル署名ｃを作成する統合デジタル署名作成手段と、前記時刻印付デジタル文書Ｍｔおよび統合デジタル署名ｃの組を時刻認証証明書（Ｍｔ，ｃ）として著者に送付する時刻認証証明書送付手段とを有することを要旨とする。

【００１６】請求項３記載の本発明にあっては、著者が作成したデジタル文書Ｍを受け取り、このデジタル文書Ｍに認証要求者が必要とする認証の有効期間情報Ｐを結合するとともにデジタル署名を作成し、更に公開鍵証明書Ｃを加えた組からなる有効期間付署名要求（ＭＰ，Ｑ，Ｃ）を送付し、この送付される有効期間付署名要求（ＭＰ，Ｑ，Ｃ）を受け取り、この要求が正規の契約者からの要求であることを検証し、検証結果が有効である場合、時刻情報ｔが有効期間Ｐに含まれるか否かを検証し、時刻情報ｔが有効期間Ｐに含まれる場合のみ、デジタル文書Ｍに時刻情報ｔを結合して時刻印付デジタル文書Ｍｔを作成し、この時刻印付デジタル文書Ｍｔを複数のデジタル署名手段に送付され、各々独立にデジタル署名を作成され、この複数のデジタル署名手段で独立に作成された複数のデジタル署名を結合して、統合デジタル署名を作成し、この統合デジタル署名および時刻印付デジタル文書の組を時刻認証証明書として著者に送付されるため、複数のデジタル署名手段による各々独自なデジタル署名により時刻印の偽造が困難であり、安全で信頼のおける時刻認証サービスが可能であるとともに、秘密鍵盗難の危険を低減することができる。また、過去に発行した時刻認証証明書を保管することもなく、記憶容量を大幅に削減し得る。更に、デジタル署名Ｑと公開鍵証明書Ｃを検証することにより、署名要求が正規の契約者であることを確認することができる。

【００１７】請求項４記載の本発明は、請求項３記載の発明において、前記時刻情報結合手段が、前記時刻印付デジタル文書Ｍｔを前記複数のデジタル署名手段に送付する時刻印付デジタル文書送付手段と、前記複数のデジタル署名手段から送付される複数のデジタル署名を受け取るデジタル署名受取手段とを有し、前記複数のデジタル署名手段の各々が、前記時刻印付デジタル文書送付手段から送付される時刻印付デジタル文書Ｍｔを受け取る時刻印付デジタル文書受取手段と、この受け取った時刻印付デジタル文書Ｍｔに対して各々独立にデジタル署名を作成するデジタル署名作成手段と、この作成されたデジタル署名を前記デジタル署名受取手段に送付する署名送付手段とを有することを要旨とする。

【００１８】請求項４記載の本発明にあっては、複数のデジタル署名手段を外部デジタル署名手段として外部に設け、結合手段からの時刻印付デジタル文書Ｍｔを時刻印付デジタル文書送付手段から外部の複数のデジタル署名手段に送付し、この複数のデジタル署名手段の各々で作成された複数のデジタル署名をデジタル署名受取手段で受け取るため、外部に設けられた複数のデジタル署名手段による各々独自なデジタル署名により時刻印の偽造が更に困難であり、安全で信頼のおける時刻認証サービスが可能である。

【００１９】また、請求項５記載の本発明は、請求項１記載の発明において、前記複数のデジタル署名手段が正常に動作しているか否を確認するための問い合わせを定期的に各デジタル署名手段に対して行い、この確認結果を前記結合手段および統合デジタル署名作成手段に供給する動作確認手段を更に有し、前記結合手段が、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書Ｍｔを送付し、前記統合デジタル署名作成手段が、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取るように構成されていることを要旨とする。

【００２０】請求項５記載の本発明にあっては、動作確認手段により各デジタル署名手段の動作を確認し、この確認結果を結合手段および統合デジタル署名作成手段に供給し、結合手段は確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書Ｍｔを送付し、統合デジタル署名作成手段は確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取るため、デジタル署名手段が悪意のある第三者により例えばメモリダンプ等を用いて秘密鍵の盗難にあっていないことを確認することができる。

【００２１】更に、請求項６記載の本発明は、請求項２記載の発明において、前記複数のデジタル署名手段が正常に動作しているか否を確認するための問い合わせを定期的に各デジタル署名手段に対して行い、この確認結果を前記時刻印付デジタル文書送付手段およびデジタル署名受取手段に供給する動作確認手段を更に有し、前記時

刻印付デジタル文書送付手段が、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書Ｍｔを送付し、前記デジタル署名受取手段が、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取るように構成されていることを要旨とする。

【００２２】請求項６記載の本発明にあっては、動作確認手段により各デジタル署名手段の動作を確認し、この確認結果を時刻印付デジタル文書送付手段およびデジタル署名受取手段に供給し、時刻印付デジタル文書送付手段は確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書Ｍｔを送付し、デジタル署名受取手段は確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取るため、デジタル署名手段が悪意のある第三者により例えばメモリダンプ等を用いて秘密鍵の盗難にあっていないことを確認することができる。

【００２３】請求項７記載の本発明は、請求項１記載の発明において、公開鍵暗号方式における公開鍵Ｋｐと秘密鍵Ｋｓの組を作成し、この作成された秘密鍵Ｋｓを分割して、前記複数のデジタル署名手段の数の数値の和として表現し、この各数値を１つずつ前記複数のデジタル署名手段の各々に配付し、配付完了後、分割前の秘密鍵を削除する鍵作成・分配手段を更に有し、前記複数のデジタル署名手段の各々が、前記鍵作成・分配手段からそれぞれ配付された秘密鍵を保持し、該秘密鍵を用いた公開鍵暗号方式で前記結合手段から配付された時刻印付デジタル文書Ｍｔに対するデジタル署名を作成し、この各デジタル署名手段からの複数のデジタル署名を前記統合デジタル署名作成手段で結合して統合デジタル署名ｃを作成し、前記時刻認証証明書送付手段で時刻印付デジタル文書Ｍｔ、統合デジタル署名ｃ、および公開鍵Ｋｐを組にして時刻認証証明書（Ｍｔ，ｃ，Ｋｐ）として著者に送付するように構成されていることを要旨とする。

【００２４】請求項７記載の本発明にあっては、鍵作成・分配手段は、公開鍵暗号方式における公開鍵Ｋｐと秘密鍵Ｋｓの組を作成し、この秘密鍵Ｋｓを分割して、複数のデジタル署名手段の数の数値の和として表現し、この各数値を１つずつ複数のデジタル署名手段の各々に配付し、配付完了後、分割前の秘密鍵を削除し、複数のデジタル署名手段の各々は、鍵作成・分配手段から配付された秘密鍵を用いた公開鍵暗号方式で時刻印付デジタル文書Ｍｔに対するデジタル署名を作成し、各デジタル署名手段からの複数のデジタル署名を結合して統合デジタル署名ｃを作成し、時刻印付デジタル文書Ｍｔ、統合デジタル署名ｃおよび公開鍵Ｋｐを組にして時刻認証証明書（Ｍｔ，ｃ，Ｋｐ）として著者に送付する。

【００２５】また、請求項８記載の本発明は、請求項７記載の発明において、前記複数のデジタル署名手段が正常に動作しているか否を確認するための問い合わせを定期的に各デジタル署名手段に対して行い、この確認結果を前記結合手段、統合デジタル署名作成手段、および鍵作成・分配手段に供給する動作確認手段を更に有し、前記鍵作成・分配手段が、動作確認手段から正常に動作していないデジタル署名手段があるという動作確認結果を受け取ると、新たな公開鍵および秘密鍵を作成し、この新たに作成した秘密鍵を前記複数のデジタル署名手段の数の和に分割し、この分割して得られた秘密鍵を各デジタル署名手段に１つずつ配付し、前記結合手段が、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書Ｍｔを送付し、この時刻印付デジタル文書Ｍｔを送付された各デジタル署名手段は前記鍵作成・分配手段から配付された秘密鍵を用いて前記結合手段から配付された時刻印付デジタル文書Ｍｔに対するデジタル署名を作成し、前記統合デジタル署名作成手段が、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取り、この受け取ったデジタル署名を前記統合デジタル署名作成手段で結合して統合デジタル署名ｃを作成し、前記時刻認証証明書送付手段で時刻印付デジタル文書Ｍｔ、統合デジタル署名ｃ、および公開鍵Ｋｐを組にして時刻認証証明書（Ｍｔ，ｃ，Ｋｐ）として著者に送付するように構成されていることを要旨とする。

【００２６】請求項８記載の本発明にあっては、鍵作成・分配手段は動作確認手段から正常に動作していないデジタル署名手段があるという動作確認結果を受け取ると、新たな公開鍵および秘密鍵を作成し、この秘密鍵をデジタル署名手段の数の和に分割し、この分割した秘密鍵を各デジタル署名手段に配付し、結合手段は正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書Ｍｔを送付し、デジタル署名手段は新たに配付された秘密鍵を用いて時刻印付デジタル文書Ｍｔに対するデジタル署名を作成し、統合デジタル署名作成手段は正常に動作しているデジタル署名手段からのみデジタル署名を受け取り、このデジタル署名を結合して統合デジタル署名ｃを作成し、時刻印付デジタル文書Ｍｔ、統合デジタル署名ｃ、および公開鍵Ｋｐを組にして時刻認証証明書（Ｍｔ，ｃ，Ｋｐ）として著者に送付するため、各デジタル署名手段の動作確認により、デジタル署名手段が悪意のある第三者によりメモリダンプ等を用いて、秘密鍵の盗難にあっていないことを確認することができ、また正常に動作していないデジタル署名手段がある場合には、新たに作成した分割秘密鍵で各デジタル署名手段が独立にデジタル署名を行うことにより、秘密鍵盗難の危険性が少なくなるとともに、時刻取得手段および各デジタル署名手段がすべて結託しない限り時刻印を偽造することができず、安全で信頼のおける時刻認証サービスを行う時刻認証外部機関を運営することができ、更

に過去に発行した時刻認証証明書を一切保管する必要がなく、従来に比較し、大幅に記憶容量を低減することができる。

【００２７】更に、請求項９記載の本発明は、請求項７記載の発明において、前記結合手段が、前記時刻印付デジタル文書Ｍｔを前記複数のデジタル署名手段に送付する時刻印付デジタル文書送付手段と、前記複数のデジタル署名手段から送付される複数のデジタル署名を受け取るデジタル署名受取手段とを有することを要旨とする。

【００２８】請求項９記載の本発明にあっては、複数のデジタル署名手段を外部デジタル署名手段として外部に設け、結合手段からの時刻印付デジタル文書Ｍｔを時刻印付デジタル文書送付手段から外部の複数のデジタル署名手段に送付し、この複数のデジタル署名手段の各々で作成された複数のデジタル署名をデジタル署名受取手段で受け取るため、外部に設けられた複数のデジタル署名手段による各々独自なデジタル署名により時刻印の偽造が更に困難であり、安全で信頼のおける時刻認証サービスが可能である。

【００２９】請求項１０記載の本発明は、請求項２記載の発明において、前記デジタル署名手段の各々が、独自に時刻情報ｔ′を取得する時刻取得手段を更に有し、前記時刻印付デジタル文書Ｍｔを受信すると、該時刻印付デジタル文書Ｍｔから直ちに時刻情報ｔを取得し、この時刻情報ｔと前記独自に取得した時刻情報ｔ′とを比較し、両者の差が所定の許容時間差以内であるときのみ、デジタル署名を作成するように構成されていることを要旨とする。

【００３０】請求項１０記載の本発明にあっては、各デジタル署名手段は、時刻印付デジタル文書Ｍｔを受信すると、該時刻印付デジタル文書Ｍｔから直ちに時刻情報ｔを取得し、この時刻情報ｔと独自に取得した時刻情報ｔ′とを比較し、両者の差が所定の許容時間差以内であるときのみ、デジタル署名を作成する。

【００３１】また、請求項１１記載の本発明は、請求項４記載の発明において、公開鍵暗号方式における公開鍵Ｋｐ２と秘密鍵Ｋｓ２の組を作成し、この作成された秘密鍵Ｋｓ２を分割して、複数のデジタル署名手段の数の数値の和として表現し、この各数値を１つずつ複数のデジタル署名手段の各々に配付し、配付完了後、分割前の秘密鍵を削除する鍵作成・分配手段を更に有し、前記時刻認証手段が、前記複数のデジタル署名手段が正常に動作しているか否を確認するための問い合わせを定期的に各デジタル署名手段に対して行う動作確認手段を更に有し、前記デジタル署名手段の各々が、独自に時刻情報ｔ′を取得する時刻取得手段を更に有し、前記時刻印付デジタル文書Ｍｔを受信すると、該時刻印付デジタル文書Ｍｔから直ちに時刻情報ｔを取得し、この時刻情報ｔと前記独自に取得した時刻情報ｔ′とを比較し、両者の差が所定の許容時間差以内であるときのみ、デジタル署名を作成するように構成され、前記鍵作成・分配手段が、前記動作確認手段から正常に動作していないデジタル署名手段があるという動作確認結果を受け取ると、新たな公開鍵および秘密鍵を作成し、この新たに作成した秘密鍵を前記複数のデジタル署名手段の数の和に分割し、この分割して得られた秘密鍵を各デジタル署名手段に１つずつ配付し、前記結合手段が、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書Ｍｔを送付し、デジタル署名手段が、時刻印付デジタル文書Ｍｔを受信すると、該時刻印付デジタル文書Ｍｔから直ちに時刻情報ｔを取得し、この時刻情報ｔと独自に取得した時刻情報ｔ′とを比較し、両者の差が所定の許容時間差以内であるときのみ、鍵作成・分配手段から配付された秘密鍵を用いて前記結合手段から配付された時刻印付デジタル文書Ｍｔに対するデジタル署名を作成し、統合デジタル署名作成手段が、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取り、この受け取ったデジタル署名を統合デジタル署名作成手段で結合して統合デジタル署名ｃを作成し、時刻認証証明書送付手段で時刻印付デジタル文書Ｍｔ、統合デジタル署名ｃ、および公開鍵Ｋｐ２を組にして時刻認証証明書（Ｍｔ，ｃ，Ｋｐ２）として著者に送付するように構成されていることを要旨とする。

【００３２】請求項１１記載の本発明にあっては、鍵作成・分配手段は動作確認手段から正常に動作していないデジタル署名手段があるという動作確認結果を受け取ると、新たな公開鍵および秘密鍵を作成し、この秘密鍵を複数のデジタル署名手段の数の和に分割し、この秘密鍵を各デジタル署名手段に配付し、結合手段は正常に動作しているデジタル署名手段のみに時刻印付デジタル文書Ｍｔを送付し、デジタル署名手段は時刻印付デジタル文書Ｍｔを受信すると、該時刻印付デジタル文書Ｍｔから直ちに時刻情報ｔを取得し、この時刻情報ｔと独自に取得した時刻情報ｔ′とを比較し、差が所定の許容時間差以内であるときのみ、鍵作成・分配手段から配付された秘密鍵を用いて時刻印付デジタル文書Ｍｔに対するデジタル署名を作成し、統合デジタル署名作成手段は正常に動作しているデジタル署名手段からのみデジタル署名を受け取り、この受け取ったデジタル署名を結合して統合デジタル署名ｃを作成し、時刻印付デジタル文書Ｍｔ、統合デジタル署名ｃ、および公開鍵Ｋｐ２を組にして時刻認証証明書（Ｍｔ，ｃ，Ｋｐ２）として著者に送付する。

【００３３】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。図１は、本発明の第１の実施形態に係る時刻認証装置の構成を示すブロック図である。同図に示す時刻認証装置において、５は著者が作成

15

したデジタル文書（Ｍ）３を受け取るデジタル文書受取手段、７は時刻を取得する時刻取得手段、９は時刻取得手段７で取得した時刻情報ｔを前記デジタル文書Ｍに結合して、１つの時刻印付デジタル文書Ｍｔを作成する結合手段、１１は結合手段９から時刻印付デジタル文書Ｍｔを受け取って、各々独立にデジタル署名を作成する複数の、本実施形態ではｓ個のデジタル署名手段、１３は複数のデジタル署名手段１１でそれぞれ独立に作成された複数のデジタル署名ｃ１，ｃ２，…，ｃｓを受け取り結合して、統合デジタル署名ｃを作成する統合デジタル署名作成手段、１５は時刻印付デジタル文書Ｍｔおよび統合デジタル署名ｃの組を時刻認証証明書（Ｍｔ，ｃ）１７として著者に送付する時刻認証証明書送付手段である。

【００３４】このように構成される時刻認証装置において、著者が作成したテキスト文書、音声情報、画像情報またはこれらの組み合わせからなるデジタル文書（Ｍ）３は、デジタル文書受取手段５で受け取られ、結合手段９に供給される。結合手段９は、時刻取得手段７を用いて時刻情報ｔを取得し、この取得した時刻情報ｔをデジタル文書Ｍに結合して、時刻印付デジタル文書Ｍｔを作成する。この時刻取得手段７が取得した時刻は、第三者が持つ正確な時計と比較して校正された正確な時計から取得することが望ましい。

【００３５】結合手段９で結合された時刻印付デジタル文書Ｍｔは、結合手段９で複数のコピーを作成し、複数のデジタル署名手段１１のすべてに送付される。この複数のデジタル署名手段１１は、それぞれ受け取った時刻印付デジタル文書Ｍｔに対して保有する秘密鍵を用いてデジタル署名ｃ１，ｃ２，…，ｃｓを作成する。

【００３６】このデジタル署名の作成例について説明する。なお、この例では公開鍵暗号の例としてＲＳＡを用いる。ＲＳＡ公開鍵暗号の説明は、辻井重雄、笠原正雄編著「暗号と情報セキュリティ」（昭晃堂）を参照する。

【００３７】ｐとｑを十分大きな素数とし、

$n = pq$

とおく。そして、$\phi(n) = (p-1)(q-1)$と互いに素な整数ｅを適当に定める。すなわち、

$gcd(e, (p-1)(q-1)) = 1$

ｎとｅを公開鍵とし、ｄを$ed = 1 \bmod \phi(n)$である整数とするとき、ｐ，ｑ，ｄを秘密鍵とする。

【００３８】時刻印付デジタル文書ＭｔにＭＤ５やＳＨＡ－１等のハッシュ関数を適用して得られるダイジェストをｍとする。更に、$c = m^d \bmod n$とおく。このとき、組（Ｍｔ，ｃ）を統合デジタル署名作成手段１３により最終的に作成される統合デジタル署名とする。図１におけるデジタル署名手段１１の和をｓとする。このとき、ｄを数の和で表現する。$d = d_1 + d_2 + \cdots + d_s$とおく。$c_1 = m^{d_1} \bmod n$，…，$c_s = m^{d_s} \bmod n$とすると、（Ｍｔ，$c_1$），…，（Ｍｔ，$c_s$）がｓ個のデジタル署名手段１１で作成されるデジタル署名となる。本実施形態では、ＲＳＡ公開鍵暗号を用いたが、楕円公開鍵暗号，ＤＳＡ（Digital Signature Algorithm）を用いても同様にデジタル署名および統合デジタル署名を作成することが可能である。

【００３９】上述したように作成された複数のデジタル署名手段１１で作成された複数のデジタル署名ｃ１，ｃ２，…，ｃｓは、各デジタル署名手段１１から統合デジタル署名作成手段１３に供給され、統合デジタル署名作成手段１３で結合され、統合デジタル署名ｃが作成される。この統合デジタル署名作成手段１３で結合作成された統合デジタル署名ｃは、時刻印付デジタル文書Ｍｔと組にされ、時刻認証証明書送付手段１５から時刻認証証明書（Ｍｔ，ｃ）１７として著者に送付される。

【００４０】上述したように、本実施形態では、複数のデジタル署名手段１１で各々独自にデジタル署名を行うため、複数のデジタル署名手段１１が協同しない限り時刻印の偽造が困難であり、安全で信頼のおける時刻認証サービスが可能であるとともに、秘密鍵盗難の危険を低減することができる。また、過去に発行した時刻認証証明書を保管することもなく、記憶容量を大幅に削減し得る。

【００４１】図２は、本発明の第２の実施形態に係る時刻認証装置の構成を示すブロック図である。

【００４２】同図に示す時刻認証装置は、図１に示した第１の実施形態の時刻認証装置における複数のデジタル署名手段１１の各々を外部デジタル署名手段１９として外部に設け、この外部デジタル署名手段１９の各々に時刻印付デジタル文書Ｍｔを送付するＭｔ送付手段２１および複数の外部デジタル署名手段１９からのデジタル署名を受け取るデジタル署名受取手段２３を設けるとともに、また各外部デジタル署名手段１９の各々を、Ｍｔ送付手段２１からの時刻印付デジタル文書Ｍｔを受け取るＭｔ受取手段２５、この受け取った時刻印付デジタル文書Ｍｔに対して独立にデジタル署名を作成する前記デジタル署名手段１１、およびこの作成されたデジタル署名をデジタル署名受取手段２３に送付する署名送付手段２７で構成している点が異なるものであり、その他の構成および作用は同じである。

【００４３】このように構成される時刻認証装置においては、著者が作成したデジタル文書（Ｍ）３は、デジタル文書受取手段５で受け取られ、結合手段９に供給される。結合手段９は、時刻取得手段７を用いて時刻情報ｔを取得し、この取得した時刻情報ｔをデジタル文書Ｍに結合して、時刻印付デジタル文書Ｍｔを作成する。

【００４４】結合手段９で結合された時刻印付デジタル文書Ｍｔは、Ｍｔ送付手段２１に供給され、Ｍｔ送付手段２１で複数のコピーを作成し、複数の外部デジタル署名手段１９のすべてに送付される。

【００４５】複数の外部デジタル署名手段１９は、それぞれＭｔ送付手段２１からの時刻印付デジタル文書Ｍｔを Ｍｔ受取手段２５で受け取り、この受け取った時刻印付デジタル文書Ｍｔをデジタル署名手段１１に供給する。デジタル署名手段１１は、時刻印付デジタル文書Ｍｔに対して保有する秘密鍵を用いてデジタル署名を作成し、署名送付手段２７に供給する。署名送付手段２７は、デジタル署名手段１１で作成されたデジタル署名をデジタル署名受取手段２３に送付する。

【００４６】デジタル署名受取手段２３は、複数の外部デジタル署名手段１９の署名送付手段２７から送付される複数のデジタル署名ｃ１，ｃ２，…，ｃｓを受け取り、統合デジタル署名作成手段１３に供給する。統合デジタル署名作成手段１３は、この複数のデジタル署名ｃ１，ｃ２，…，ｃｓを結合して、統合デジタル署名ｃを作成する。この統合デジタル署名作成手段１３で結合作成された統合デジタル署名ｃは、時刻印付デジタル文書Ｍｔと組にされ、時刻認証証明書送付手段１５から時刻認証証明書（Ｍｔ，ｃ）１７として著者に送付される。

【００４７】本実施形態では、複数の外部デジタル署名手段１９で各々独自にデジタル署名を行うため、複数の外部デジタル署名手段１９が協同しない限り時刻印の偽造が困難であり、安全で信頼のおける時刻認証サービスが可能である。

【００４８】図３は、本発明の第３の実施形態に係る時刻認証装置の構成を示すブロック図である。

【００４９】同図に示す時刻認証装置は、図１に示した時刻認証装置に対して有効期間付き署名要求を行う機能を設けた点が異なるものであり、図１に示した時刻認証装置に相当する機能に有効期間付き署名を検証する有効期間付署名検証手段３１および時刻情報ｔが有効期間Ｐに含まれるか否かを検証する有効期間内時刻情報検証手段３３を付加した時刻認証部３５と、著者からデジタル文書（Ｍ）３を受け取り、このデジタル文書（Ｍ）３に有効期間Ｐを結合し、更にこの結合されたデジタル文書Ｍと有効期間Ｐに対してデジタル署名Ｑを作成し、このＭＰ，Ｑ、および時刻認証部３５から供給される公開鍵証明書Ｃを組にして有効期間付署名要求（ＭＰ，Ｑ，Ｃ）として時刻認証部３５に送付する有効期間付き署名要求部３７とを有する。なお、時刻認証部３５は、有効期間付署名検証手段３１および有効期間内時刻情報検証手段３３に加えて、デジタル文書受取手段５および時刻認証証明書送付手段１５しか図示されていないが、実際には、これらに加えて、図１の構成と同じように時刻取得手段７、結合手段９、複数のデジタル署名手段１１、および統合デジタル署名作成手段１３も有しているものである。

【００５０】有効期間付き署名要求部３７は、予め公開鍵暗号方式における公開鍵Ｋｐと秘密鍵Ｋｓを作成して保持しており、この作成された公開鍵Ｋｐを時刻認証部３５に送付するようになっている。また、時刻認証部３５は、この有効期間付き署名要求部３７から送付された公開鍵Ｋｐに対するデジタル署名を時刻認証部３５の秘密鍵Ｋｓ' で作成し、公開鍵Ｋｐと作成されたデジタル署名を組にした公開鍵証明書Ｃを有効期間付き署名要求部３７に返送するようになっている。

【００５１】そして、有効期間付き署名要求部３７は、著者からのデジタル文書（Ｍ）３を受け取るデジタル文書受取手段３９、この受け取ったデジタル文書Ｍを署名要求者が設定した時刻認証部３５が時刻認証を行うことが可能な有効期間Ｐと結合する結合手段４１、この結合されたデジタル文書Ｍと有効期間ＰからなるＭＰに対して秘密鍵Ｋｓを用いてデジタル署名Ｑを作成するデジタル署名手段４３、デジタル文書Ｍと有効期間Ｐの結合されたＭＰ、デジタル署名Ｑ、および時刻認証部３５から受け取った公開鍵証明書Ｃを組にして有効期間付署名要求として時刻認証部３５に送付する有効期間付署名要求送付手段４５から構成されている。

【００５２】次に、以上のように構成される時刻認証装置の作用を説明する。著者が作成したデジタル文書（Ｍ）３を有効期間付き署名要求部３７のデジタル文書受取手段３９で受け取り、結合手段４１に送付する。署名要求者は、時刻認証部３５が時刻認証を行うことが可能な有効期間Ｐを設定し、結合手段４１は、デジタル文書受取手段３９を介して受け取ったデジタル文書Ｍと有効期間Ｐを結合し、デジタル署名手段４３に送付する。デジタル署名手段４３は、ＭＰに対して秘密鍵Ｋｓを用いてデジタル署名Ｑを作成する。有効期間付署名要求送付手段４５は、デジタル文書Ｍと有効期間Ｐの結合されたＭＰ、デジタル署名Ｑ、および公開鍵証明書Ｃを組にして有効期間付署名要求として時刻認証部３５に送付する。

【００５３】時刻認証部３５は、この有効期間付署名要求（ＭＰ，Ｑ，Ｃ）デジタル文書受取手段５で受け取ると、この有効期間付署名要求（ＭＰ，Ｑ，Ｃ）に含まれる公開鍵証明書Ｃが上述したように事前に時刻認証部３５が発行した公開鍵証明書Ｃであるか否かを時刻認証部３５の公開鍵Ｋｐ' を用いて有効期間付署名検証手段３１で検証する。すなわち、時刻認証部３５の公開鍵を用いて公開鍵証明書Ｃを復号し、その結果得られた公開鍵Ｋｐを用いてデジタル署名Ｑを復号した結果がＭＰと一致することを検証することにより有効期間付署名要求（ＭＰ，Ｑ，Ｃ）が時刻認証部３５の正規の契約者らかの要求であることを確認する。

【００５４】デジタル署名Ｑが、通常公開鍵デジタル署名で行われているように、ＭＰにハッシュ関数を適用した結果に対して、秘密鍵Ｋｓを用いて作成されている場合には、デジタル署名Ｑを復号して得られる結果がＭＰにハッシュ関数を適用して結果と一致することを検証する。

【００５５】更に、時刻認証部３５は、有効期間内時刻情報検証手段３３を用いて、時刻情報ｔが有効期間Ｐに含まれることを確認することにより、有効期間付署名要求（ＭＰ，Ｑ，Ｃ）が今から有効期間Ｐ以内に作成されたものであることを検証する。

【００５６】また、時刻認証部３５は、上述したように、図１に示したと同じ構成を有しているので、有効期間付き署名要求部３７から受け取った有効期間付署名要求（ＭＰ，Ｑ，Ｃ）に含まれるデジタル文書Ｍを結合手段９に供給し、結合手段９は時刻取得手段７から取得した時刻情報ｔをデジタル文書Ｍに結合して、時刻印付デジタル文書Ｍｔを作成する。この時刻印付デジタル文書Ｍｔは、結合手段９で複数のコピーを作成し、複数のデジタル署名手段１１のすべてに送付される。この複数のデジタル署名手段１１は、それぞれ受け取った時刻印付デジタル文書Ｍｔに対して保有する秘密鍵を用いてデジタル署名ｃ１，ｃ２，…，ｃｓを作成する。

【００５７】複数のデジタル署名手段１１で作成された複数のデジタル署名ｃ１，ｃ２，…，ｃｓは、各デジタル署名手段１１から統合デジタル署名作成手段１３に供給され、統合デジタル署名作成手段１３で結合され、統合デジタル署名ｃが作成される。この統合デジタル署名ｃは、時刻印付デジタル文書Ｍｔと組にされ、時刻認証証明書送付手段１５から時刻認証証明書（Ｍｔ，ｃ）１７として著者に送付される。このように、複数のデジタル署名手段で各々独自にデジタル署名を行うため、時刻印の偽造が困難であり、安全で信頼のおける時刻認証サービスが可能である。

【００５８】なお、上記実施形態においては、時刻認証部３５は、図１に示した時刻認証装置に対して有効期間付署名検証手段３１および有効期間内時刻情報検証手段３３を付加した構成のものであると説明したが、図１に示した時刻認証装置の代わりに図２に示したように複数のデジタル署名手段１１が外部に設けられ、各々がＭｔ受取手段２５、デジタル署名手段１１、署名送付手段２７からなる複数の外部デジタル署名手段１９を有する図２の時刻認証装置を用いてもよいものである。

【００５９】図４は、本発明の第４の実施形態に係る時刻認証装置の構成を示すブロック図である。

【００６０】同図に示す時刻認証装置は、図３に示した第３の実施形態の時刻認証装置における複数のデジタル署名手段１１の各々を外部デジタル署名手段１９として外部に設け、この外部デジタル署名手段１９の各々に時刻印付デジタル文書Ｍｔを送付するＭｔ送付手段２１および複数の外部デジタル署名手段１９からのデジタル署名を受け取るデジタル署名受取手段２３を時刻認証部３５に設けている点が異なるものであり、その他の構成および作用は図３に示した第３の実施形態と同じであるので、その説明は省略する。

【００６１】図５は、本発明の第５の実施形態に係る時刻認証装置の構成を示すブロック図である。同図に示す時刻認証装置は、図１に示した第１の実施形態の時刻認証装置において複数のデジタル署名手段１１の動作を確認する動作確認手段４９を設けた点が異なるのみであり、その他の構成および作用は図１の時刻認証装置と同じである。

【００６２】動作確認手段４９は、定期的に複数のデジタル署名手段１１の動作を確認するための問い合わせを各デジタル署名手段１１に対して行い、一定時間以内に応答があるデジタル署名手段１１が正常に動作していると判定し、この判定結果を結合手段９および統合デジタル署名作成手段１３に供給するようになっている。また、結合手段９は、動作確認手段４９からの判定結果に従って正常に動作しているデジタル署名手段１１にのみ時刻印付デジタル文書Ｍｔを送付し、統合デジタル署名作成手段１３は、正常に動作しているデジタル署名手段１１からのみデジタル署名を受け取るようになっている。

【００６３】このように各デジタル署名手段１１の動作を確認することにより、デジタル署名手段１１が悪意のある第三者によりメモリダンプ等を用いて、秘密鍵の盗難にあっていないことを確認することができる。正常動作していないと判定されたデジタル署名手段１１がある場合には、その判定結果を結合手段９および統合デジタル署名作成手段１３に通知する。正常と判定されたデジタル署名手段１１は新たな秘密鍵を保持する。結合手段９および統合デジタル署名作成手段１３は、正常動作していると判定されたデジタル署名手段１１だけからのデジタル署名を用いて統合デジタル署名ｃを作成する。

【００６４】図６は、本発明の第６の実施形態に係る時刻認証装置の構成を示すブロック図である。同図に示す時刻認証装置は、図２に示した第２の実施形態の時刻認証装置に図５に示した動作確認手段４９を設けたものであり、具体的には図２に示した第２の実施形態の時刻認証装置において外部に設けた複数の外部デジタル署名手段１９の動作を確認する動作確認手段４９を設けた点が異なるのみであり、その他の構成および作用は図１の時刻認証装置と同じである。

【００６５】動作確認手段４９は、定期的に複数の外部デジタル署名手段１９の動作を確認するための問い合わせを各外部デジタル署名手段１９に対して行い、一定時間以内に応答がある外部デジタル署名手段１９が正常に動作していると判定し、この判定結果をＭｔ送付手段２１およびデジタル署名受取手段２３に供給するようになっている。

【００６６】また、Ｍｔ送付手段２１は、動作確認手段４９からの判定結果に従って正常に動作している外部デジタル署名手段１９にのみ時刻印付デジタル文書Ｍｔを送付し、デジタル署名受取手段２３は、正常に動作しているデジタル署名手段１１からのみデジタル署名を受け

取るようになっている。

【００６７】このように各外部デジタル署名手段１９の動作を確認することにより、図５に示した第５の実施形態の場合と同様に、外部デジタル署名手段１９が悪意のある第三者によりメモリダンプ等を用いて、秘密鍵の盗難にあっていないことを確認することができる。

【００６８】図７は、本発明の第７の実施形態に係る時刻認証装置の構成を示すブロック図である。同図に示す時刻認証装置は、図１に示した第１の実施形態の時刻認証装置に対して鍵作成・分配手段５１を設けた点が異なるものであり、その他の構成および作用は同じである。

【００６９】鍵作成・分配手段５１は、公開鍵暗号方式における公開鍵Ｋｐと秘密鍵Ｋｓの組を作成し、この作成された秘密鍵Ｋｓを分割して、デジタル署名手段１１の数であるｓ個（ｓ＞１）の数値の和として表現し、この各数値を１つずつｓ個のデジタル署名手段１１に配付し、配付完了後、分割前の秘密鍵Ｋｓを削除する機能を有する。

【００７０】複数のデジタル署名手段１１の各々は、鍵作成・分配手段５１からそれぞれ配付された秘密鍵を保持し、前記結合手段９から配付された時刻印付デジタル文書Ｍｔに対して該秘密鍵を用いて公開鍵暗号方式を用いたデジタル署名ｃ１，ｃ２，…，ｃｓを作成する。

【００７１】このように作成された複数のデジタル署名ｃ１，１ｃ２，…，ｃｓは、各デジタル署名手段１１から統合デジタル署名作成手段１３に供給され、統合デジタル署名作成手段１３で結合され、統合デジタル署名ｃが作成される。この統合デジタル署名ｃは、時刻認証証明書送付手段１５に供給され、時刻認証証明書送付手段１５は、時刻印付デジタル文書Ｍｔ、統合デジタル署名ｃ、および公開鍵Ｋｐを組にして、時刻認証証明書（Ｍｔ，ｃ，Ｋｐ）として著者に送付する。

【００７２】図８は、本発明の第８の実施形態に係る時刻認証装置の構成を示すブロック図である。同図に示す時刻認証装置は、図７に示した第７の実施形態の時刻認証装置において図５の実施形態と同様に複数のデジタル署名手段１１の動作を確認する動作確認手段４９を設けた点が異なるのみであり、その他の構成および作用は図１の時刻認証装置と同じである。

【００７３】動作確認手段４９は、図５の実施形態で説明したと同様に、定期的に複数のデジタル署名手段１１の動作を確認するための問い合わせを各デジタル署名手段１１に対して行い、一定時間以内に応答があるデジタル署名手段１１が正常に動作していると判定し、この判定結果を結合手段９および統合デジタル署名作成手段１３に供給するようになっていることに加えて、動作確認手段４９は各デジタル署名手段１１の動作確認の結果、正常に動作していないデジタル署名手段１１が１つでもあると判定した場合には、この判定結果を結合手段９、統合デジタル署名作成手段１３に加えて鍵作成・分配手段５１にも供給するようになっている。

【００７４】そして、鍵作成・分配手段５１は、動作確認手段４９から正常に動作していないデジタル署名手段１１が１つでもあるという判定結果を受け取った場合には、新たな公開鍵Ｋｐおよび秘密鍵Ｋｓを作成し、この作成された秘密鍵Ｋｓを正常に動作していることを確認したデジタル署名手段１１の数の和に分割する。そして、この分割して得られた秘密鍵を正常と判定されたデジタル署名手段１１の各々の１つずつ配付する。配付後、分割前の秘密鍵を削除する。正常と判定された各デジタル署名手段１１は、新たに配付された秘密鍵を保持する。

【００７５】また、結合手段９は、動作確認手段４９から判定結果の通知を受け取ると、鍵作成・分配手段５１が上述したようにデジタル署名手段１１に配付した後、正常と判定されたデジタル署名手段１１にのみ時刻印付デジタル文書Ｍｔを送付する。

【００７６】また、結合手段９は、動作確認手段４９からの判定結果に従って正常に動作しているデジタル署名手段１１にのみ時刻印付デジタル文書Ｍｔを送付し、統合デジタル署名作成手段１３は、正常に動作しているデジタル署名手段１１からのみデジタル署名を受け取るようになっている。デジタル署名手段１１は、新たに配付された秘密鍵を用いて時刻印付デジタル文書Ｍｔに対してデジタル署名を作成する。統合デジタル署名作成手段１３も同様に、正常と判定されたデジタル署名手段１１からのみデジタル署名を受け取り、この受け取ったデジタル署名のみを使用して統合デジタル署名ｃを作成する。この統合デジタル署名ｃは、時刻認証証明書送付手段１５に供給され、時刻認証証明書送付手段１５は、時刻印付デジタル文書Ｍｔ、統合デジタル署名ｃ、および公開鍵Ｋｐを組にして、時刻認証証明書（Ｍｔ，ｃ，Ｋｐ）として著者に送付する。

【００７７】このように各デジタル署名手段１１の動作を確認することにより、デジタル署名手段１１が悪意のある第三者によりメモリダンプ等を用いて、秘密鍵の盗難にあっていないことを確認することができる。また、動作確認手段４９により各デジタル署名手段１１の動作確認を行い、正常に動作していないデジタル署名手段１１がある場合には、新たな公開鍵Ｋｐおよび秘密鍵Ｋｓを作成し、この作成された秘密鍵Ｋｓを正常に動作しているデジタル署名手段１１の数の和に分割し、この分割により得られた秘密鍵を正常と判定されたデジタル署名手段１１の各々に１つずつ配付し、正常と判定されたデジタル署名手段１１からのみ時刻印付デジタル文書Ｍｔに対するデジタル署名を受け取るようにするとともに、また複数のデジタル署名手段１１が秘密鍵を分割して所有し、それぞれのデジタル署名手段１１が独立にデジタル署名を行うことにより、秘密鍵盗難の危険性を少なくするとともに、時刻を取得する手段とデジタル署名を行

う手段を実行するすべての機関が結託しない限り時刻印を偽造することができず、安全で信頼のおける時刻認証サービスを行う時刻認証外部機関を運営することができる。また、過去に発行した時刻認証証明書を一切保管する必要がなく、従来に比較し、大幅に記憶容量を低減することができる。

【００７８】図９は、本発明の第９の実施形態に係る時刻認証装置の構成を示すブロック図である。同図に示す時刻認証装置は、図７に示した第７の実施形態の時刻認証装置において複数のデジタル署名手段１１の各々を外部デジタル署名手段１９として外部に設け、この外部デジタル署名手段１９の各々に時刻印付デジタル文書Ｍｔを送付するＭｔ送付手段２１および複数の外部デジタル署名手段１９からのデジタル署名を受け取るデジタル署名受取手段２３を設けた点が異なるのみであり、その他の構成および作用は図７の実施形態と同じであるので、その説明は省略する。

【００７９】図１０は、本発明の第１０の実施形態に係る時刻認証装置の構成を示すブロック図である。同図に示す時刻認証装置は、図４に示した第４の実施形態の時刻認証装置において、時刻認証部３５に動作確認手段４９を設けるとともに、鍵作成・分配手段５１を設け、更に各外部デジタル署名手段１９をＭｔ受取手段２５および署名送付手段２７に加えて、時刻正当性判定手段５５を設けた点が異なるのみであり、その他の構成および作用は図４と同じである。

【００８０】各外部デジタル署名手段１９に設けられた時刻正当性判定手段５５は、各外部デジタル署名手段１９がＭｔ送付手段２１から受け取った時刻印付デジタル文書Ｍｔに付加されている時刻情報ｔと各外部デジタル署名手段１９で独自に取得した時刻情報ｔ′とを比較し、両者の差が十分小さい場合に限り、各外部デジタル署名手段１９において鍵作成・分配手段５１で既に作成された秘密鍵を用いて時刻印付デジタル文書Ｍｔに対するデジタル署名を作成し、この作成したデジタル署名を署名送付手段２７が時刻認証部３５のデジタル署名受取手段２３に送付するように構成されているものである。

【００８１】更に詳しくは、本実施形態において、有効期間付き署名要求部３７の有効期間付署名要求送付手段４５からは著者の公開鍵Ｋｐが添付されている有効期間付署名要求（ＭＰ，Ｑ，Ｋｐ，Ｃ）を時刻認証部３５に送付するようになっている。Ｃを時刻認証部３５の公開鍵K_p'で復号して得られるＫｐを用いてＱがＭＰのデジタル署名になっていることを検証する代わりに、（ＭＰ，Ｑ，Ｋｐ，Ｃ）に含まれるＫｐを用いてＱを復号した結果がＭＰになっていること、およびＣを時刻認証部３５の公開鍵K_p'で復号してＫｐが得られることを検証する。デジタル署名Ｑが、ＭＰにハッシュ関数を適用した結果に対して、秘密鍵Ｋｓを用いて作成されている場合には、デジタル署名Ｑを復号して得られる結果がＭＰにハッシュ関数を適用して結果と一致することを検証する。

【００８２】時刻認証部３５に設けられた動作確認手段４９は、上述したと同様に、複数の外部デジタル署名手段１９が正常に動作しているか否かの動作確認を定期的に行い、正常に動作していない外部デジタル署名手段１９が１つでもある場合には、鍵作成・分配手段５１に新たな公開鍵Ｋｐ２および秘密鍵Ｋｓ２の作成を依頼する。鍵作成・分配手段５１は、この依頼に応じて新たな公開鍵Ｋｐ２および秘密鍵Ｋｓ２を作成し、この秘密鍵Ｋｓを正常に動作している外部デジタル署名手段１９の数の和に分割し、この分割して得られた秘密鍵を正常に動作している各外部デジタル署名手段１９に１つずつ配付する。

【００８３】一方、時刻認証部３５のデジタル文書受取手段５は、有効期間付き署名要求部３７から有効期間付署名要求（ＭＰ，Ｑ，Ｋｐ，Ｃ）を受け取ると、この時に時刻取得手段７から時刻情報ｔを取得する。それから、図３および図４に示した実施形態と同じ検証を行い、検証の結果、有効と判定された有効期間付署名要求（ＭＰ，Ｑ，Ｋｐ，Ｃ）からデジタル文書Ｍを取り出し、この取り出したデジタル文書Ｍに先に取得した時刻情報ｔを結合手段９で結合する。そして、この結合した時刻印付デジタル文書Ｍｔをｔ送付手段２１から正常に動作している外部デジタル署名手段１９に送付する。外部デジタル署名手段１９は、この受け取った時刻印付デジタル文書Ｍｔに付加されている時刻情報ｔと外部デジタル署名手段１９が先に取得した時刻情報ｔ′と比較し、両者の差が十分小さい場合に限り、鍵作成・分配手段５１で既に作成した秘密鍵を用いて、時刻印付デジタル文書Ｍｔに対するデジタル署名を作成し、この作成したデジタル署名を署名送付手段２７から時刻認証部３５のデジタル署名受取手段２３に送付する。

【００８４】デジタル署名受取手段２３は、各外部デジタル署名手段１９からのデジタル署名を受け取り、統合デジタル署名作成手段１３に供給する。統合デジタル署名作成手段１３は、各デジタル署名を結合して、統合デジタル署名ｃを作成する。時刻認証証明書送付手段１５は、時刻印付デジタル文書Ｍｔ、統合デジタル署名ｃ、および公開鍵Ｋｐ２を組にして時刻認証証明書（Ｍｔ，ｃ，Ｋｐ）として著者に送付する。

【００８５】

【発明の効果】以上説明したように、本発明によれば、著者が作成したデジタル文書Ｍは時刻情報ｔを結合されて、時刻印付デジタル文書Ｍｔが作成され、この時刻印付デジタル文書Ｍｔは複数のデジタル署名手段に送付され、各々独立にデジタル署名を作成され、この複数のデジタル署名手段で独立に作成された複数のデジタル署名を結合して、統合デジタル署名を作成し、この統合デジタル署名および時刻印付デジタル文書の組を時刻認証証

明書として著者に送付されるので、複数のデジタル署名手段による各々独自なデジタル署名により時刻印の偽造が困難であり、安全で信頼のおける時刻認証サービスが可能であるとともに、秘密鍵盗難の危険を低減することができる。また、過去に発行した時刻認証証明書を保管することもなく、記憶容量を大幅に削減し得る。

【００８６】また、本発明によれば、複数のデジタル署名手段を外部デジタル署名手段として外部に設け、時刻印付デジタル文書Ｍｔを外部の複数のデジタル署名手段に送付し、この複数のデジタル署名手段の各々で作成された複数のデジタル署名をデジタル署名受取手段で受け取るので、外部に設けられた複数のデジタル署名手段による各々独自なデジタル署名により時刻印の偽造が更に困難であり、安全で信頼のおける時刻認証サービスが可能である。

【００８７】更に、本発明によれば、著者が作成したデジタル文書Ｍを受け取り、このデジタル文書Ｍに認証要求者が必要とする認証の有効期間情報Ｐを結合するとともにデジタル署名を作成し、更に公開鍵証明書Ｃを加えた組からなる有効期間付署名要求（ＭＰ，Ｑ，Ｃ）を送付し、この送付される有効期間付署名要求（ＭＰ，Ｑ，Ｃ）を受け取り、この要求が正規の契約者からの要求であることを検証し、検証結果が有効である場合、時刻情報ｔが有効期間Ｐに含まれるか否かを検証し、時刻情報ｔが有効期間Ｐに含まれる場合のみ、デジタル文書Ｍに時刻情報ｔを結合して時刻印付デジタル文書Ｍｔを作成し、この時刻印付デジタル文書Ｍｔを複数のデジタル署名手段に送付され、各々独立にデジタル署名を作成され、この複数のデジタル署名手段で独立に作成された複数のデジタル署名を結合して、統合デジタル署名を作成し、この統合デジタル署名および時刻印付デジタル文書の組を時刻認証証明書として著者に送付されるので、複数のデジタル署名手段による各々独自なデジタル署名により時刻印の偽造が困難であり、安全で信頼のおける時刻認証サービスが可能であるとともに、秘密鍵盗難の危険を低減することができ、また過去に発行した時刻認証証明書を保管することもなく、記憶容量を大幅に削減でき、更にデジタル署名Ｑと公開鍵証明書Ｃを検証することにより、署名要求が正規の契約者であることを確認することができる。

【００８８】本発明によれば、動作確認手段により各デジタル署名手段の動作を確認し、この確認結果を結合手段および統合デジタル署名作成手段に供給し、結合手段は確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書Ｍｔを送付し、統合デジタル署名作成手段は確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取るので、デジタル署名手段が悪意のある第三者により例えばメモリダンプ等を用いて秘密鍵の盗難にあっていないことを確認することができる。

【００８９】また、本発明によれば、鍵作成・分配手段は動作確認手段から正常に動作していないデジタル署名手段があるという動作確認結果を受け取ると、新たな公開鍵および秘密鍵を作成し、この秘密鍵をデジタル署名手段の数の和に分割し、この秘密鍵を各デジタル署名手段に配付し、正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書Ｍｔを送付し、デジタル署名手段は新たに配付された秘密鍵を用いて時刻印付デジタル文書Ｍｔに対するデジタル署名を作成し、正常に動作しているデジタル署名手段からのみデジタル署名を受け取り、このデジタル署名を結合して統合デジタル署名ｃを作成し、時刻印付デジタル文書Ｍｔ、統合デジタル署名ｃ、および公開鍵Ｋｐを組にして時刻認証証明書（Ｍｔ，ｃ，Ｋｐ）として著者に送付するので、各デジタル署名手段の動作確認により、デジタル署名手段が悪意のある第三者によりメモリダンプ等を用いて、秘密鍵の盗難にあっていないことを確認することができ、また正常に動作していないデジタル署名手段がある場合には、新たに作成した分割秘密鍵で各デジタル署名手段が独立にデジタル署名を行うことにより、秘密鍵盗難の危険性が少なくなるとともに、時刻取得手段および各デジタル署名手段がすべて結託しない限り時刻印を偽造することができず、時刻認証外部機関が１つの秘密鍵を用いてデジタル署名を行う場合の秘密鍵の盗難の危険性や著者と時刻認証外部機関が結託して過去にさかのぼって時刻印を押す偽造の危険性を排除することができ、安全で信頼のおける時刻認証サービスを行う時刻認証外部機関を運営することができ、更に過去に発行した時刻認証証明書を一切保管する必要がなく、従来に比較し、大幅に記憶容量を低減することができ、また更にデジタル署名と公開鍵証明書を検証することにより、署名要求が正規の契約者であることを確認することができ、正規の契約者以外の者が不正に時刻認証サービスを受けることを防止することができる。

【００９０】更に、本発明によれば、各デジタル署名手段は時刻印付デジタル文書Ｍｔを受信すると、該時刻印付デジタル文書Ｍｔから直ちに時刻情報ｔを取得し、この時刻情報ｔと独自に取得した時刻情報ｔ′とを比較し、両者の差が所定の許容時間差以内であるときのみ、デジタル署名を作成する。

【００９１】本発明によれば、鍵作成・分配手段は動作確認手段から正常に動作していないデジタル署名手段があるという動作確認結果を受け取ると、新たな公開鍵および秘密鍵を作成し、この秘密鍵を複数のデジタル署名手段の数の和に分割し、この秘密鍵を各デジタル署名手段に配付し、正常に動作しているデジタル署名手段のみに時刻印付デジタル文書Ｍｔを送付し、デジタル署名手段は時刻印付デジタル文書Ｍｔを受信すると、該時刻印付デジタル文書Ｍｔから直ちに時刻情報ｔを取得し、この時刻情報ｔと独自に取得した時刻情報ｔ′とを比較

し、差が所定の許容時間差以内であるときのみ、鍵作成・分配手段から配付された秘密鍵を用いて時刻印付デジタル文書Ｍｔに対するデジタル署名を作成し、統合デジタル署名作成手段は正常に動作しているデジタル署名手段からのみデジタル署名を受け取り、この受け取ったデジタル署名を結合して統合デジタル署名ｃを作成し、時刻印付デジタル文書Ｍｔ、統合デジタル署名ｃ、および公開鍵Ｋｐ２を組にして時刻認証証明書（Ｍｔ，ｃ，Ｋｐ２）として著者に送付するので、各デジタル署名手段の動作確認により、デジタル署名手段が悪意のある第三者によりメモリダンプ等を用いて、秘密鍵の盗難にあっていないことを確認することができ、また正常に動作していないデジタル署名手段がある場合には、新たに作成した分割秘密鍵で各デジタル署名手段が独立にデジタル署名を行うことにより、秘密鍵盗難の危険性が少なくなるとともに、時刻取得手段および各デジタル署名手段がすべて結託しない限り時刻印を偽造することができず、時刻認証外部機関が１つの秘密鍵を用いてデジタル署名を行う場合の秘密鍵の盗難の危険性や著者と時刻認証外部機関が結託して過去にさかのぼって時刻印を押す偽造の危険性を排除することができ、安全で信頼のおける時刻認証サービスを行う時刻認証外部機関を運営することができ、更に過去に発行した時刻認証証明書を一切保管する必要がなく、従来に比較し、大幅に記憶容量を低減することができ、また更にデジタル署名と公開鍵証明書を検証することにより、署名要求が正規の契約者であることを確認することができ、正規の契約者以外の者が不正に時刻認証サービスを受けることを防止することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係る時刻認証装置の構成を示すブロック図である。

【図２】本発明の第２の実施形態に係る時刻認証装置の構成を示すブロック図である。

【図３】本発明の第３の実施形態に係る時刻認証装置の構成を示すブロック図である。

【図４】本発明の第４の実施形態に係る時刻認証装置の構成を示すブロック図である。

【図５】本発明の第５の実施形態に係る時刻認証装置の構成を示すブロック図である。

【図６】本発明の第６の実施形態に係る時刻認証装置の構成を示すブロック図である。

【図７】本発明の第７の実施形態に係る時刻認証装置の構成を示すブロック図である。

【図８】本発明の第８の実施形態に係る時刻認証装置の構成を示すブロック図である。

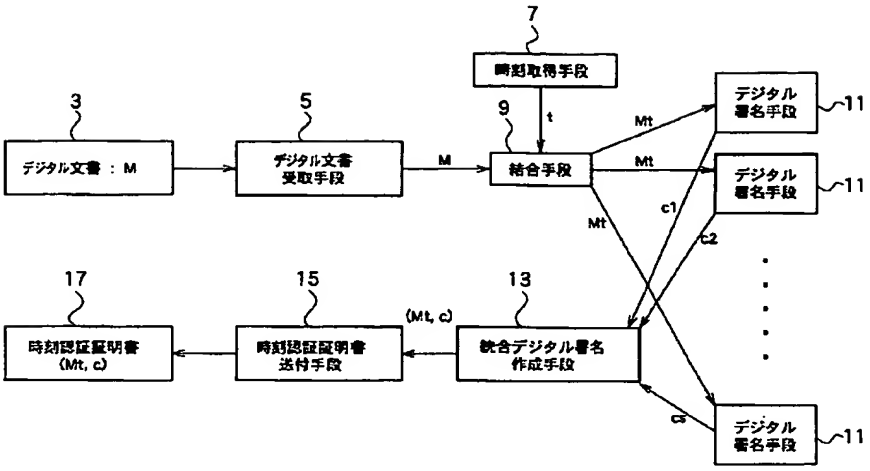
【図９】本発明の第９の実施形態に係る時刻認証装置の構成を示すブロック図である。

【図１０】本発明の第１０の実施形態に係る時刻認証装置の構成を示すブロック図である。

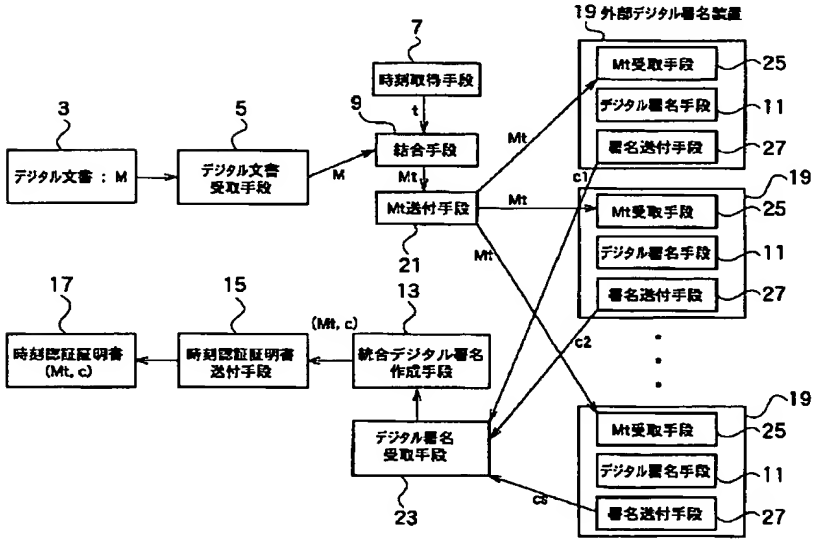
【符号の説明】

５　デジタル文書受取手段
７　時刻取得手段
９　結合手段
１１　デジタル署名手段
１３　統合デジタル署名作成手段
１５　時刻認証証明書送付手段
１９　外部デジタル署名手段
２１　Ｍｔ送付手段
２３　デジタル署名受取手段
３１　有効期間付署名検証手段
３３　有効期間内時刻情報検証手段
３５　時刻認証部
３７　有効期間付き署名要求部
４５　有効期間付署名要求送付手段
４９　動作確認手段
５１　鍵作成・分配手段
５５　時刻正当性判定手段

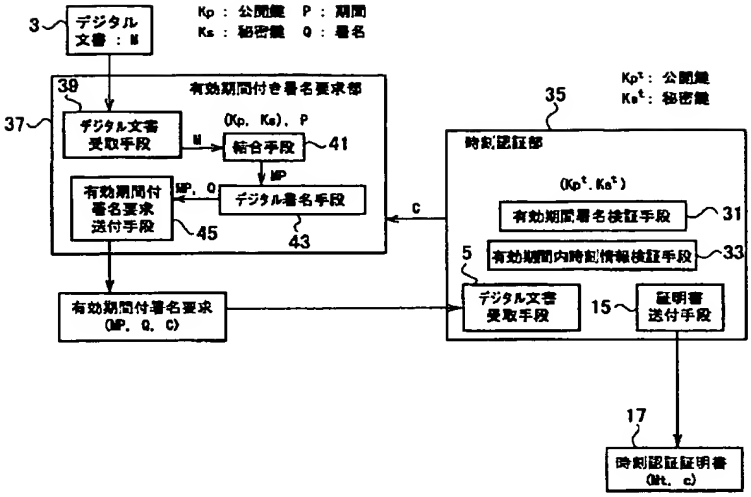
【図１】


7
時刻取得手段
3
デジタル文書：M
5
デジタル文書受取手段
M
9
t
結合手段
Mt
デジタル署名手段
11
c1
c2
cs
17
時刻認証証明書(Mt, c)
15
時刻認証証明書送付手段
(Mt, c)
13
統合デジタル署名作成手段

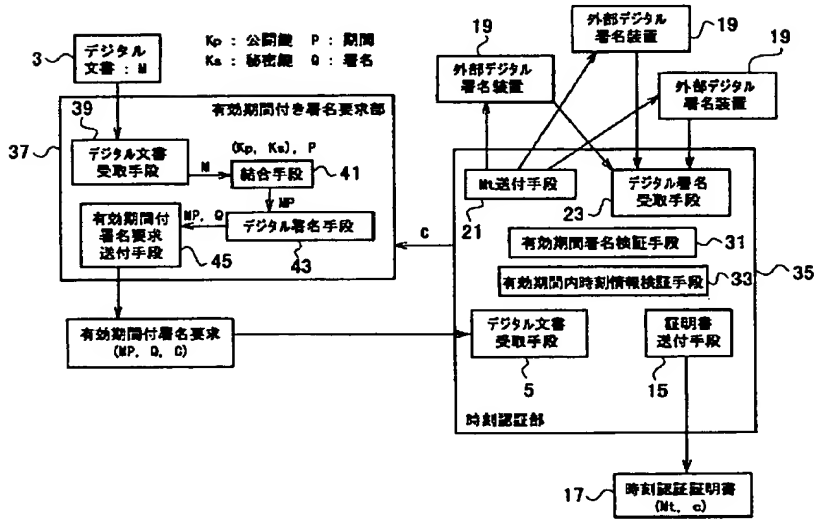
【図２】


19 外部デジタル署名装置
7
時刻取得手段
3
デジタル文書：M
5
デジタル文書受取手段
9
t
結合手段
M
Mt
Mt送付手段
21
Mt受取手段
25
デジタル署名手段
11
署名送付手段
27
c1
c2
cs
17
時刻認証証明書(Mt, c)
15
時刻認証証明書送付手段
(Mt, c)
13
統合デジタル署名作成手段
デジタル署名受取手段
23

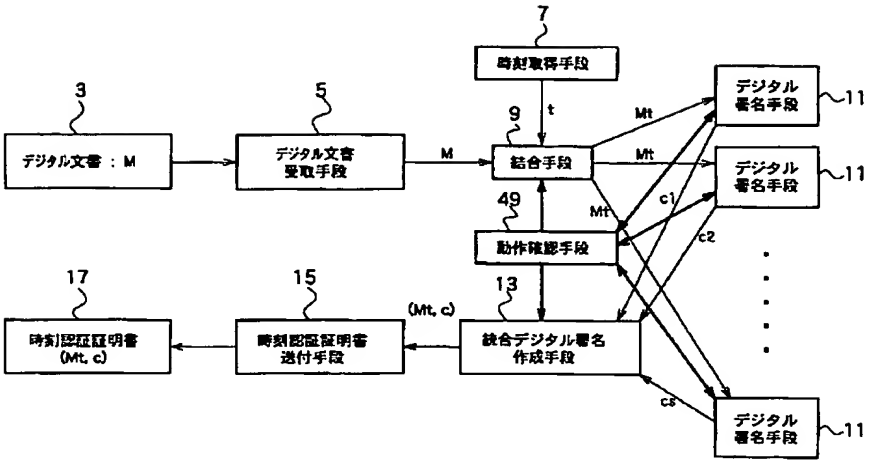
【図３】


3
デジタル文書：M
Kp：公開鍵 P：期間
Ks：秘密鍵 Q：署名
39
有効期間付き署名要求部
37
デジタル文書受取手段
M
(Kp, Ks), P
結合手段
41
MP
有効期間付署名要求送付手段
MP, Q
デジタル署名手段
45
43
C
35
Kp^t：公開鍵
Ks^t：秘密鍵
時刻認証部
(Kp^t, Ks^t)
有効期間署名検証手段
31
5
有効期間内時刻情報検証手段
33
デジタル文書受取手段
15
証明書送付手段
有効期間付署名要求 (MP, Q, C)
17
時刻認証証明書 (Mt, c)

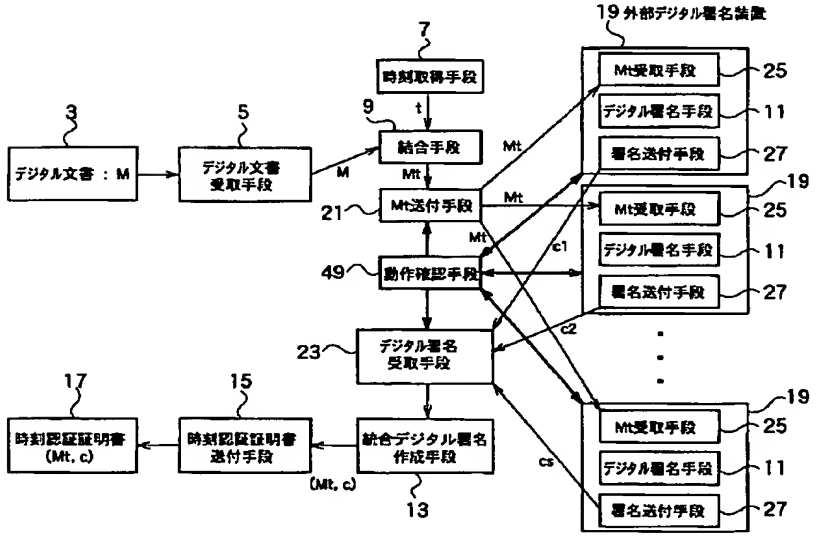
【図４】


3
デジタル文書：M
Kp：公開鍵 P：期間
Ks：秘密鍵 Q：署名
19
外部デジタル署名装置
19
外部デジタル署名装置
19
外部デジタル署名装置
39
有効期間付き署名要求部
37
デジタル文書受取手段
M
(Kp, Ks), P
結合手段
41
MP
有効期間付署名要求送付手段
MP, Q
デジタル署名手段
45
43
C
Mt送付手段
21
デジタル署名受取手段
23
有効期間署名検証手段
31
有効期間内時刻情報検証手段
33
35
有効期間付署名要求 (MP, Q, C)
デジタル文書受取手段
5
証明書送付手段
15
時刻認証部
17
時刻認証証明書 (Mt, c)

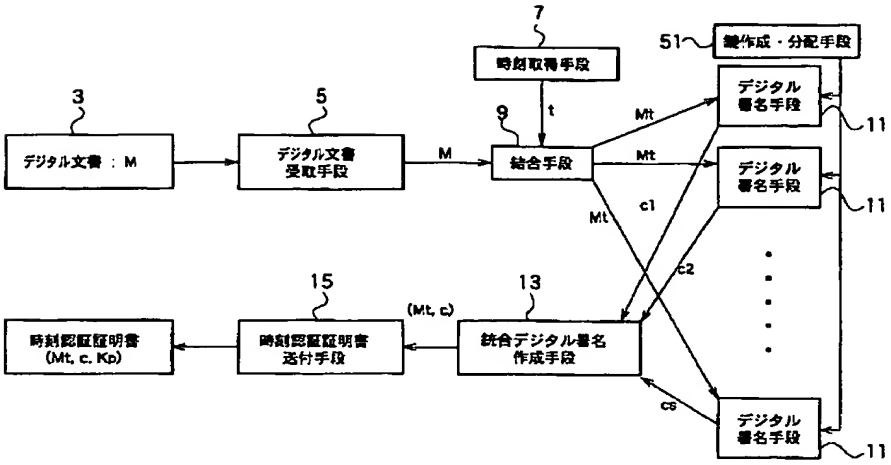
【図５】


7
時刻取得手段
3
デジタル文書：M
5
デジタル文書
受取手段
M
9
t
結合手段
Mt
デジタル
署名手段
11
c1
c2
49
動作確認手段
17
時刻認証証明書
(Mt, c)
15
時刻認証証明書
送付手段
(Mt, c)
13
統合デジタル署名
作成手段
cs

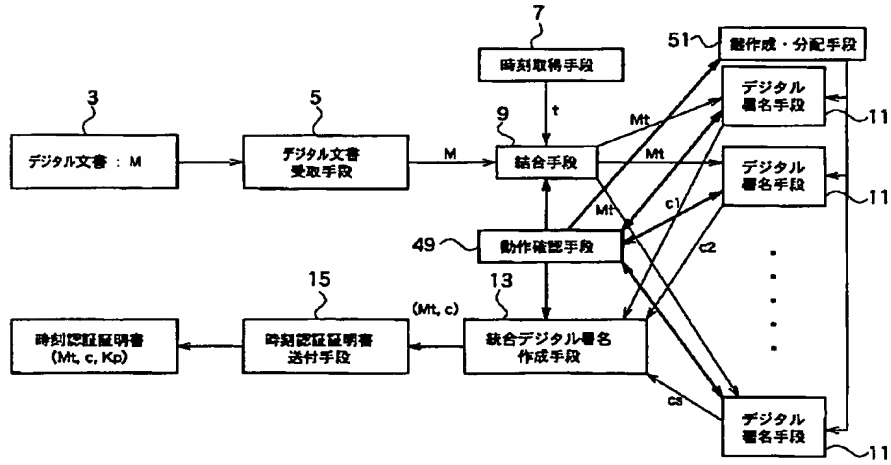
【図６】


19 外部デジタル署名装置
7
時刻取得手段
3
デジタル文書：M
5
デジタル文書
受取手段
9
t
結合手段
Mt
M
21
Mt送付手段
49
動作確認手段
23
デジタル署名
受取手段
17
時刻認証証明書
(Mt, c)
15
時刻認証証明書
送付手段
(Mt, c)
13
統合デジタル署名
作成手段
Mt受取手段
25
デジタル署名手段
11
署名送付手段
27
c1
c2
cs

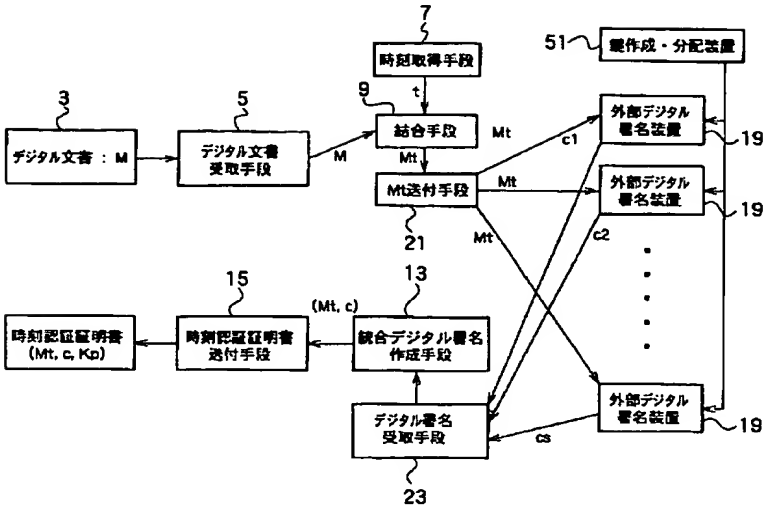
【図７】


7
時刻取得手段
51
鍵作成・分配手段
3
デジタル文書：M
5
デジタル文書
受取手段
M
9
結合手段
t
Mt
Mt
Mt
c1
c2
cs
デジタル
署名手段
11
15
時刻認証証明書
送付手段
(Mt, c)
13
統合デジタル署名
作成手段
時刻認証証明書
(Mt, c, Kp)

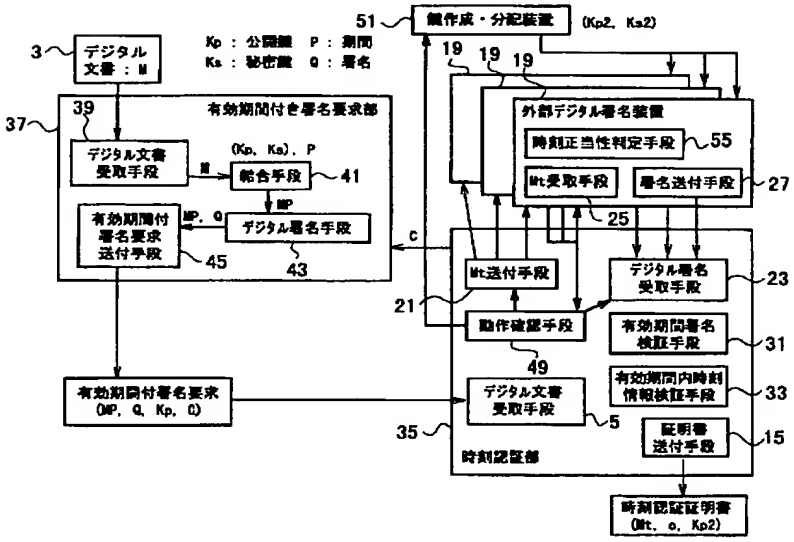
【図８】


7
時刻取得手段
51
鍵作成・分配手段
3
デジタル文書：M
5
デジタル文書
受取手段
M
9
結合手段
t
Mt
Mt
Mt
c1
c2
cs
デジタル
署名手段
11
49
動作確認手段
15
時刻認証証明書
送付手段
(Mt, c)
13
統合デジタル署名
作成手段
時刻認証証明書
(Mt, c, Kp)

【図９】


7
時刻取得手段
51
鍵作成・分配装置
3
デジタル文書：M
5
デジタル文書受取手段
9
t
結合手段
Mt
M
Mt
Mt送付手段
21
外部デジタル署名装置
19
c1
c2
cs
15
時刻認証証明書送付手段
13
(Mt, c)
統合デジタル署名作成手段
時刻認証証明書 (Mt, c, Kp)
デジタル署名受取手段
23

【図１０】


51
鍵作成・分配装置
(Kp2, Ks2)
3
デジタル文書：M
Kp：公開鍵　P：期間
Ks：秘密鍵　Q：署名
19
外部デジタル署名装置
時刻正当性判定手段
55
Mt受取手段
署名送付手段
27
25
37
39
有効期間付き署名要求部
デジタル文書受取手段
(Kp, Ks), P
結合手段
41
有効期間付署名要求送付手段
MP, Q
デジタル署名手段
45
43
c
Mt送付手段
21
デジタル署名受取手段
23
動作確認手段
49
有効期間署名検証手段
31
有効期間内時刻情報検証手段
33
有効期間付署名要求 (MP, Q, Kp, c)
デジタル文書受取手段
5
35
証明書送付手段
15
時刻認証部
時刻認証証明書 (Mt, c, Kp2)